Hard Fork

Origem: Wikipédia, a enciclopédia livre.

[Saltar para a navegação](https://pt.wikipedia.org/wiki/Hard_Fork#mw-head)[Saltar para a pesquisa](https://pt.wikipedia.org/wiki/Hard_Fork#p-search)

No contexto das [criptomoedas](https://pt.wikipedia.org/wiki/Criptomoeda), um [*fork*](https://pt.wikipedia.org/wiki/Fork) pode ser definido como aquilo que ocorre quando uma [*blockchain*](https://pt.wikipedia.org/wiki/Blockchain) divide-se em dois caminhos distintos que coexistem de modo paralelo,[[1]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-1) similar por exemplo ao que ocorre em sistemas de controle de versão como o [Git](https://pt.wikipedia.org/wiki/Git) onde um repositório pode possuir várias cópias distintas que existem de forma simultânea e podem ser alteradas sem afetar nenhuma das outras.

Um fork ocasionalmente ocorre no processo de mineração de criptomoedas, quando dois mineradores encontram um novo bloco ao mesmo tempo, fazendo com que a rede se divida temporariamente. Posteriormente, o software da *blockchain* fará com que o conflito seja resolvido e a rede volte a um estado unificado. Contudo, um [fork](https://pt.wikipedia.org/wiki/Fork) também pode ser provocado pelos próprios desenvolvedores e mantenedores de uma criptomoeda no momento em que eles decidem que as regras de validação de transações atuais devem sofrer algum tipo de alteração.[[2]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-2)

Tal tipo de alteração nas regras de validação pode gerar dois tipos de *fork*, o *soft fork* e o *hard fork*.[[3]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-3) O primeiro tipo pode ser definido como uma mudança no conjunto de regras que permite que blocos criados pelo novo conjunto de regras continuem sendo válidos. Utilizando uma metáfora simples no contexto de computação, um *soft fork* pode ser comparado a uma atualização mais simples de um sistema operacional de um computador que adiciona algumas funcionalidades mas que não é drástica o suficiente para que o número principal da versão seja alterado.[[4]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-4) Já o *hard fork* poderia ser comparada ao lançamento de uma nova versão *major* de um sistema operacional, como quando usuários migram do Windows 7 para o Windows 8 e pode haver algum tipo de mudança nas regras de funcionamento dos mesmos que inviabilize que algum programa que executava anteriormente execute no novo, e vice-versa. Ou seja, em um *hard fork*, blocos criados com as novas regras passam a não ser válidos de acordo com a regra antiga, sendo criada "do zero" uma nova *blockchain* que passa a atender às novas regras da criptomoeda, com as regras antigas continuando a existir na versão prévia. Um *hard fork* mal realizado, contudo, poderia levar à total inutilização da *blockchain* de uma criptomoeda.

**Índice**

  [esconder]

* [1Definição](https://pt.wikipedia.org/wiki/Hard_Fork#Defini%C3%A7%C3%A3o)
* [2Bitcoin Cash](https://pt.wikipedia.org/wiki/Hard_Fork#Bitcoin_Cash)
* [3Bitcoin Gold](https://pt.wikipedia.org/wiki/Hard_Fork#Bitcoin_Gold)
* [4Bitcoin Diamond](https://pt.wikipedia.org/wiki/Hard_Fork#Bitcoin_Diamond)
* [5SegWit2x](https://pt.wikipedia.org/wiki/Hard_Fork#SegWit2x)
* [6Futuros Hard Forks](https://pt.wikipedia.org/wiki/Hard_Fork#Futuros_Hard_Forks)
* [7Referências](https://pt.wikipedia.org/wiki/Hard_Fork#Refer%C3%AAncias)

Definição[[editar](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&veaction=edit&section=1" \o "Editar secção: Definição) | [editar código-fonte](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&action=edit&section=1)]

Um *hard fork* pode ser implementado com a intenção de corrigir algum tipo de falha de segurança presente em alguma versão da criptomoeda, quando tal modificação torna inválidos blocos que anteriormente eram válidos. Ainda pode ocorrer para que novas funcionalidades sejam acrescentadas à *blockchain* ou então para reverter alguma transação realizada (conforme ocorreu após a invasão à *blockchain* da rede [Ethereum](https://pt.wikipedia.org/wiki/Ethereum).

No caso do ataque ao *Ethereum* citado acima, o *hard fork* fez com que as transações fraudulentas fossem invalidadas. Isso ocorreu no momento em que houve a divergência no fluxo da *blockchain* à partir dos nós que não foram atualizados para o novo conjunto de regras protocolares do *software*. Após a invasão ao sistema da criptomoeda, os membros da comunidade do *Ethereum* decidiram favoravelmente, de forma quase unânime, que deveria ser realizado um *hard fork* de modo a invalidar e cancelar as transações fraudulentas, responsáveis por um prejuízo de dezenas de milhões de dólares válidos em moedas digitais, causadas por um *hacker* anônimo. O *hard fork* realizado permitiu que os membros da rede que possuiam *tokens* pudessem reaver seus fundos em *ether*.

A proposta da comunidade, no caso, não desfez todo o histórico de transações da rede. Ao invés disso, o que ocorreu foi uma realocação dos fundos atrelados ao sistema para um novo tipo de [Contrato Inteligente](https://pt.wikipedia.org/wiki/Contrato_Inteligente) cujo único propósito era permitir que os usuários tivessem a possibilidade de reaver suas criptomoedas.[[5]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-5)

Bitcoin Cash[[editar](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&veaction=edit&section=2" \o "Editar secção: Bitcoin Cash) | [editar código-fonte](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&action=edit&section=2)]

Um exemplo de criptomoeda gerada à partir de um hard fork é o [Bitcoin Cash](https://pt.wikipedia.org/wiki/Bitcoin_Cash), criado em 1 de agosto de 2017 como um derivado da famosa criptomoeda [Bitcoin](https://pt.wikipedia.org/wiki/Bitcoin).[[6]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-6) O *Bitcoin Cash* adota um protocolo alternativo em relação à sua antecessora, que visa aumentar a capacidade de uma transação realizada.[[7]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-7) Isso é possível pois o *Bitcoin Cash* possui um tamanho diferenciado para seus blocos, atingindo um valor padrão de 8MB,[[8]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-8) sendo maior que o original proposto por [Satoshi Nakamoto](https://pt.wikipedia.org/wiki/Satoshi_Nakamoto), com planos para expansão ainda maior desse valor no futuro.[[9]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-9) Esse maior espaço visa proporcionar um auxílio na correção do problema relacionado à escalabilidade da criptomoeda que afetava a criptomoeda original, sendo uma solução alternativa ao *SegWit* (*Seggregated Witness*) adotado pelo *Bitcoin*, que é considerada uma otimização polêmica a ser aplicada na *blockchain*.[[10]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-10)

Tal polêmica estava no fato de alguns membros da comunidade do *Bitcoin* imaginarem que a adoção no novo protocolo favoreceria àqueles que desejavam utilizar a criptomoeda como uma forma de investimento digital e não como uma forma de realizar transações alternativa à tradicional usando moedas reais.[[11]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-11) Após a realização da bifurcação, todas as transações realizadas anteriormente no *Bitcoin* tradicional foram herdadas, mas todas as transações subsequentes passaram a ser próprias da nova criptomoeda, sendo o primeiro bloco único ao *Bitcoin Cash* o de número 478558.[[12]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-12)

Além disso, os desenvolvedores do *Bitcoin Cash* citam a chamada "parede invisível" causada pelo limite de 1MB dos blocos do *Bitcoin* como um fator que prejudicava a usabilidade da criptomoeda, citando que alguns usuários chegavam a aguardar dias para terem suas transações confirmadas e um dos motivos para realizar a divergência na *blockchain*.[[13]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-13)

Bitcoin Gold[[editar](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&veaction=edit&section=3" \o "Editar secção: Bitcoin Gold) | [editar código-fonte](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&action=edit&section=3)]

Outro exemplo de criptomoeda gerada por *hard fork* do *Bitcoin* é o [Bitcoin Gold](https://pt.wikipedia.org/w/index.php?title=Bitcoin_Gold&action=edit&redlink=1), criado por [Jack Liao](https://pt.wikipedia.org/w/index.php?title=Jack_Liao&action=edit&redlink=1). A ideia por trás dessa criptomoeda é a de tentar resolver a questão da centralização dos mineradores de *Bitcoin* realizando melhorias na forma como é implementada a [Prova de Trabalho](https://pt.wikipedia.org/wiki/Prova_de_Trabalho).[[14]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-14) A prova de trabalho escolhida pelos desenvolvedores do *Bitcoin Gold* foi a da modalidade [Equihash](https://pt.wikipedia.org/w/index.php?title=Equihash&action=edit&redlink=1), um algoritmo usado também pela [ZCash](https://pt.wikipedia.org/w/index.php?title=ZCash&action=edit&redlink=1) que é um outro tipo de criptomoeda, e que é bastante resistente aos ASICs, que são circuitos integrados que realizam apenas uma atividade específica. A ideia de adotar essa tecnologia é permitir que os usuários utilizem tanto recursos de [CPU](https://pt.wikipedia.org/wiki/CPU) quanto de [GPU](https://pt.wikipedia.org/wiki/GPU) nos processos de mineração dos recursos. Um processo de prova de trabalho que adota o *Equihash*, efetivamente, é beneficiado pela quantidade de [Memória RAM](https://pt.wikipedia.org/wiki/Mem%C3%B3ria_RAM) que o usuário possui em sua máquina.[[15]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-15)

A principal razão de o *Bitcoin Gold* adotar uma modalidade de prova de trabalho que seja resistente aos ASICs está no fato de o cenário de mineração de criptomoedas estar bastante dominado por esse tipo de equipamento. Isso acontece pois geralmente o processo de prova de trabalho estar associado a uma função criptográfica relativamente simples e que não requer muito poder computacional, um cenário perfeito para tais dispositivos operarem. O *Equihash*, por outro lado, exige uma capacidade computacional bastante elevada, não sendo acessível economicamente construir um ASIC que seja especializado em minerar *Bitcoin Gold*.

Bitcoin Diamond[[editar](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&veaction=edit&section=4" \o "Editar secção: Bitcoin Diamond) | [editar código-fonte](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&action=edit&section=4)]

O [Bitcoin Diamond](https://pt.wikipedia.org/w/index.php?title=Bitcoin_Diamond&action=edit&redlink=1) é mais uma divergência do *Bitcoin* original, lançado em 24 de novembro de 2017 e tendo como bloco base na *blockchain* o de número 495866.[[16]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-16) É uma criptomoeda do tipo POW X13 GPU, necessitando ser minerado utilizando um processador gráfico ao invés de uma CPU, com uma oferta na ordem das 210 milhões de unidades, exatamente dez vezes mais que o *Bitcoin*. O tamanho dos blocos do *Bitcoin Diamond* é de 8MB e os mesmos são gerados a cada 10 minutos.[[17]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-17)

Os desenvolvedores da criptomoeda são listados no site da mesma como um trio composto por "EVEY", "007" e "?", porém não são informados maiores detalhes acerca dos mesmos. De acordo com o Forex Magnates, tanto "EVEY" quanto "007" são conhecidos, ou ainda grupos de, mineradores de *Bitcoin* que operam na China e são completamente responsáveis pelo desenvolvimento do *Bitcoin Diamond*.[[18]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-18)

SegWit2x[[editar](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&veaction=edit&section=5) | [editar código-fonte](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&action=edit&section=5)]

O [SegWit2x](https://pt.wikipedia.org/wiki/SegWit2x) foi uma proposta de *hard fork* do *Bitcoin* original que estava previsto para ser lançado em novembro de 2017 mas que foi cancelada por não ter conseguido trazer um consenso para dentro da comunidade de usuários quando da atualização dos blocos, o que de acordo com os desenvolvedores poderia ser responsável por segregar ainda mais a comunidade do *Bitcoin*.[[19]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-19)

A ideia original da criptomoeda foi lançada em maio de 2017 como uma forma de aprimorar a usabilidade e a escalabilidade do *Bitcoin*, numa época em que a comunidade estava em constantes debates acerca do futuro da criptomoeda. Em agosto do mesmo ano, o [SegWit](https://pt.wikipedia.org/w/index.php?title=SegWit&action=edit&redlink=1) foi uma implementação bem sucedida do chamado [Acordo de Nova Iorque](https://pt.wikipedia.org/w/index.php?title=Acordo_de_Nova_Iorque&action=edit&redlink=1), no qual aqueles que desejavam aumentar o tamanho efetivo dos blocos da *blockchain* chegaram a um acordo com aqueles que desejavam aumentar o tamanho do bloco através de um *hard fork*, que veio a ser a segunda etapa do projeto. A ideia é que o aumento realizado modificasse o tamanho do bloco para 2MB, o que fez com que algumas companhias que apoiavam o acordo original mudassem de posicionamento, com a bifurcação em novembro podendo causar a criação de mais uma *blockchain* além da do *Bitcoin Cash*.[[20]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-20)

Apesar do cancelamento do *SegWit2x*, um grupo de desenvolvedores ameaçou prosseguir com o *fork* independentemente da decisão, porém uma série de erros no repositório do código impediu que a ação fosse concretizada.[[21]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-21) Um dos bugs em particular apontava que o bloco esperado para a ocorrência do *fork* era o de 494783, porém o bloco que havia sido informado oficialmente como esperado era o de número 494784, o que acabou fazendo com que o algoritmo ficasse preso no bloco errôneo.

Futuros Hard Forks[[editar](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&veaction=edit&section=6" \o "Editar secção: Futuros Hard Forks) | [editar código-fonte](https://pt.wikipedia.org/w/index.php?title=Hard_Fork&action=edit&section=6)]

O sucesso proporcionado por essas divergências na *blockchain* gerou uma grande atração nos desenvolvedores, que iniciaram os procedimentos para a criação de novos forks a partir do *Bitcoin*. Estão previstas cinco novas criptomoedas derivadas para serem lançadas ainda em dezembro de 2017, com três dessas inclusive já tendo definido qual será o bloco da *blockchain* a partir do qual ocorrerá a separação. Os novos *hard forks* são o [Super Bitcoin](https://pt.wikipedia.org/w/index.php?title=Super_Bitcoin&action=edit&redlink=1), que tem como ponto de partida na *blockchain* original o bloco 498888, o [Bitcoin Platinum](https://pt.wikipedia.org/w/index.php?title=Bitcoin_Platinum&action=edit&redlink=1) a partir do 500000 e o [Bitcoin Cash Plus](https://pt.wikipedia.org/w/index.php?title=Bitcoin_Cash_Plus&action=edit&redlink=1) que será originado do bloco 501407. Ainda estão previstos, mas sem bloco base definido, outros dois *hard forks*, o [Bitcoin Uranium](https://pt.wikipedia.org/w/index.php?title=Bitcoin_Uranium&action=edit&redlink=1) e o [Bitcoin Silver](https://pt.wikipedia.org/w/index.php?title=Bitcoin_Silver&action=edit&redlink=1).[[22]](https://pt.wikipedia.org/wiki/Hard_Fork" \l "cite_note-22)

É sempre importante salientar que o principal ponto para que uma criptomoeda seja considera bem-sucedida é a sua aceitação por parte da comunidade de usuários e também por parte das empresas que trabalham com criptomoedas, sendo necessário haver empresas da área que sejam confiáveis o suficiente para fornecer serviços de qualidade ao público como carteiras para as moedas e meios de liquidez.[[23]](https://pt.wikipedia.org/wiki/Hard_Fork#cite_note-23)